PURPOSE

This protocol supports Bay of Plenty District Health Board (BOPDHB) policy 2.6.2 and sets out the standards expected from staff when using the BOPDHB email system.

STANDARDS TO BE MET

1. Use of the BOPDHB email system by staff is permitted and encouraged when it is being used appropriately for business purposes and supports the goals and objectives of the BOPDHB.
2. Staff should not set any automatic forwarding of BOPDHB business emails to personal private emails addresses, and email correspondence associated with business purposes should be conducted via the BOPDHB email system.
3. Email access shall be controlled through individual accounts and passwords. Each user of the BOPDHB's email system is required to read and acknowledge that he / she has read this Email Usage policy prior to receiving an email access account and password.
4. Email accounts will not be provided to non BOPDHB employees except under exceptional circumstances where authorised by the General Manager Information Management or approved delegate.
5. Unless other arrangements are made, email access is to be terminated when an employee leaves the employ of the BOPDHB. The organisation is under no obligation to store or forward the contents of an individual's email inbox / outbox after their employment has ceased.
6. Email should be used as part of the normal execution of an employee's responsibilities and should be used in a manner that is consistent with the BOPDHB's standards of business conduct and professional and personal courtesy.
7. Information communicated via email should be subject to the same protocols and publication standards as traditional means of communication (e.g. confidentiality, approval by Manager, review by appropriate higher levels). Users should exercise caution when communicating confidential or sensitive information via email.
8. Any email messages sent outside of the organisation must include the organisation's standard confidentiality statement (note this is automatically added).
9. The email system and services used at BOPDHB remain the property of BOPDHB and the organisation reserves the right to monitor the volume and cost of email traffic generated by each person at all times, and the right to monitor, retrieve and read all communication in the following circumstances:
   9.1 Legitimate business need (e.g. routine system administration, access to information when the employee is unavailable but timing is critical).
   9.2 Reasonable suspicion of prohibited activities.

   Information obtained in these circumstances may be disclosed to direct managers of staff members involved and other authorities if necessitated by the information retrieved.
10. The email system and services are not to be used in a way that could be reasonably expected to cause excessive strain on the organisation's network and information systems. The BOPDHB reserves the right to filter file attachments on incoming and outgoing emails based on file size or type. Further, the organisation reserves the right to limit the size of users' email mailboxes.

11. Staff should not send or receive any information protected by copyright unless permission has been officially provided. Users must abide by all software licensing agreements, copyright laws and other applicable regulations.
12. Staff using email must ensure that the use they make is 'appropriate'. This includes but is not limited to:
    - 12.1 Conducting research and investigation in support of output delivery.
    - 12.2 Communication and information exchange with government agencies and other organisations as required by business (if relevant).
    - 12.3 Receiving news stories or other information of interest to the organisation.
    - 12.4 Professional development activity, such as maintaining currency with and/or debating issues in a field of knowledge. This includes personal development activity, such as university associations and professional societies.
13. Communication within the organisation that is business related and/or supports the goals and objectives of the BOPDHB.
14. Staff must not use email for inappropriate purposes as this may be deemed as serious misconduct. Inappropriate purposes include, but are not limited to:
    - 14.1 Receiving communications that contain material that is obscene, objectionable, likely to be offensive or which contains "adult content".
    - 14.2 Soliciting for personal gain or profit.
    - 14.3 Making or posting indecent remarks and proposals.
    - 14.4 Receiving any software without gaining approval from the IT department.
    - 14.5 Passing off personal views as representing those of the organisation.
    - 14.6 Any activity that violates New Zealand law and / or codes of conduct.
    - 14.7 Extensive private usage.
    - 14.8 Using the email to harass, defame, denigrate either another employee or a third party.
    - 14.9 Electronic greeting cards (e-cards).
15. Unless sanctioned under this protocol, no employee shall view, copy, alter or delete emails and / or email accounts of another employee or a third party.
16. Employees must not share, nor attempt to obtain another employee's, passwords, user identification or other secure information. Sharing of logins puts the login owner at risk if another user uses their login inappropriately. BOPDHB reserves the right to withdraw system access from users who persist in sharing their passwords and logins.
17. If an employee receives an email containing material that they believe is offensive, the onus is on the employee to communicate their concerns or views to the sender asking that such material not be sent to them, and also inform their Manager and / or Information Technology (IT) department.
18. Email users are responsible for accessing their mail boxes in a timely fashion so as to meet their business and role oriented tasks, and for the management of their mailboxes, including organisation and clearing.
19. Where relevant to an employee's duties, remote access to BOPDHB email is provided to via secure Webmail. Such access to be approved by the employee's manager.
20. Synchronised email onto mobile devices is only permitted where the device is approved for business use by the employee's manager, and where the mobile device is managed by the provided BOPDHB security toolset as per protocol 2.6.6 P2 . BOPDHB email synchronisation is not permitted onto computers which are not managed by the BOPDHB IT Department.

21. Email users are responsible for maintaining the volume of email and attachments held in their individual mail boxes, including ensuring that the size does not unreasonably impact the operation of the email system.
22. Email users are responsible for ensuring that any e-mail message that is a "business record" is managed in accordance with relevant legislation and retention standards.
23. Email users are responsible for adhering to the email related requirements of 2.6.2 P4 Sensitive Data and 2.6.6 P2 Mobile Device Acceptable Use and Security.
24. The IT department is responsible for implementing appropriate email archiving capabilities to enable users to manage the storage and retention of emails that constitute business records and manage the size of their mail boxes.
25. Access to another employee's mailbox may be granted by the General Manager Information Management or approved delegate when required for business continuity purposes.
26. Any breach of this protocol will be investigated and may be subject to actions including but not limited to one or more of the following:
    - 26.1 Temporary and permanent revocation of email access.
    - 26.2 Investigation and disciplinary action under policy 3.50.02 protocol 9 Investigation Process and 3.50.02 protocol 15 Disciplinary Process.
    - 26.3 Legal action according to applicable laws and contractual arrangements.

ASSOCIATED DOCUMENTS

- Bay of Plenty District Health Board policy 2.6.2 Digital Communication
- Bay of Plenty District Health Board policy 2.6.2.protocol 2 Internet Usage
- Bay of Plenty District Health Board policy 2.6.2.protocol 3 Social Media
- Bay of Plenty District Health Board policy 2.6.2.protocol 4 Sensitive Data
- Bay of Plenty District Health Board policy 2.6.2 protocol 5 Cloud Services
- Bay of Plenty District Health Board policy 3.50.13 Investigation and Disciplinary